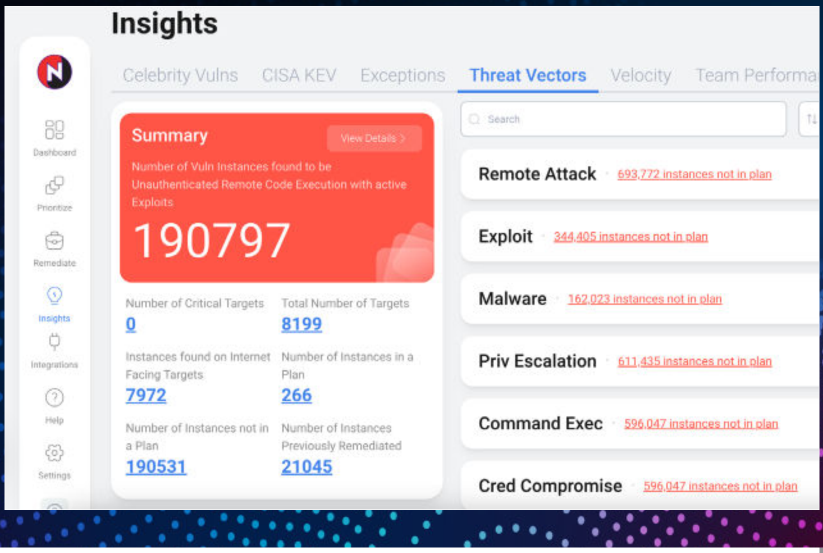
Solution Brief

NOPSEC

Jumpstarting CTEM for Media & Entertainment

Three critical capabilities to overcome vulnerability and threat response gridlock



Insights

Summary

Number of Vuln Instances found to be Unauthenticated Remote Code Execution with active Exploits

190797

Number of Critical Targets 0	Total Number of Targets 8199
Instances found on Internet Facing Targets 7972	Number of Instances in a Plan 266
Number of Instances not in a Plan 190531	Number of Instances Previously Remediated 21045

Remote Attack	693,772 instances not in plan
Exploit	344,405 instances not in plan
Malware	162,023 instances not in plan
Priv Escalation	611,435 instances not in plan
Command Exec	596,047 instances not in plan
Cred Compromise	596,047 instances not in plan

67%
Of customers improved program maturity in 6 months or less with NopSec

As a CISO in the Media and Entertainment (M&E) industry, you must continuously mature your security organization to keep pace with the ever-evolving threat landscape. You aim to implement the continuous threat exposure management (CTEM) progress, as defined by Gartner, to accomplish this. To do this successfully means more than just increasing the number of vulnerabilities your teams remediate. It requires you to become the change agent for your organization and shift your organization's mindset from being task centric to risk centric.

Unfortunately, your teams' perpetual vulnerability and threat overload holds you back from making this evolution. This common challenge prevents shifting your teams' focus from vulnerabilities to exposures, an essential first step toward CTEM. However, there are clear steps you can take today to jumpstart your CTEM program and resolve this hurdle. The first step is understanding why your teams are overwhelmed and its impact.

The Challenge: Most SecOps teams are in gridlock

Today's reality is an overwhelming volume of vulnerabilities and threats paralyzes prioritization efforts. Your teams, mainly relying on makeshift tools and spreadsheets, are mired in reactive whack-a-mole vulnerability and threat response.

For CISOs like you, two primary factors compound the challenge:

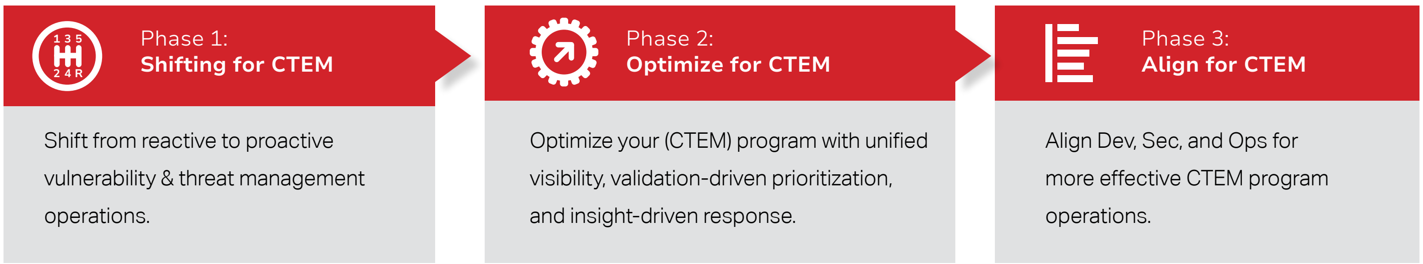
- **Complex Mitigation Decisions**: Managing data across diverse security systems, scanners, and controls creates gaps. Further, patching is a nuanced practice influenced by workloads, risk appetite, and business directives. As you've probably heard often, "When we're rendering, nothing takes down our systems."
- **Diverse Architectures, Unified Challenges:** Different business units with unique architectures (e.g., hard shell/soft center, honeycomb) make unified vulnerability and threat response challenging, requiring precise control over self-service management.

> **"When we're rendering, nothing takes down our systems."**
>
> - Global Studio Itops Director

The challenge is clear. Your teams are in gridlock, accentuated by poor data integrity and communication, a lack of context, and disjointed vulnerability and threat response. Overcoming this gridlock must happen before embarking on a CTEM journey.

The CTEM operationalization roadmap to success

Successfully implementing a CTEM program requires a platform that delivers the core capabilities that effectively change CTEM from a paper exercise into a real-world operation. NopSec calls this alignment process Operationalizing for CTEM. This is a three-phase process to remove the hurdles of today and make way for CTEM tomorrow (see Figure 1). The first of these phases is – Shifting for CTEM.



Phase 1:
Shifting for CTEM

Shift from reactive to proactive vulnerability & threat management operations.

Phase 2:
Optimize for CTEM

Optimize your (CTEM) program with unified visibility, validation-driven prioritization, and insight-driven response.

Phase 3:
Align for CTEM

Align Dev, Sec, and Ops for more effective CTEM program operations.

Figure 1 – Operationalizing for CTEM

Jumpstarting your journey by shifting

Jumpstarting your CTEM journey requires overcoming operational gridlock by shifting from reactive vulnerability management to proactive. As the originator of the Cyber Threat Exposure Management (CTEM) Platform, NopSec delivers three fundamental capabilities (see Table 1) to make this happen:

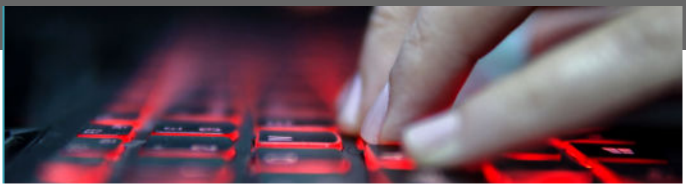
UNIFIED VISIBILITY | **PROACTIVE PRIORITIZATION** | **INSIGHTFUL RESPONSE**

Together, these capabilities give your teams the headroom necessary to break through the gridlock and shift to more proactive operations: the first step toward operationalizing a CTEM program.

Challenge	• Gaps in coverage • Data overload and duplication • Reliance on spreadsheets	• Whack-a-mole vulnerability management • Inability to make informed patching decisions • Reactive response to new threats and vulnerabilities	• Inability to support multiple stakeholders • Decision paralysis due to insufficient analysis
Solution	**Unified Visibility** • Establish a unified view of your IT, security, and service landscape, consolidating all vulnerability and threat data	**Proactive Prioritization** • Utilizing machine learning to prioritize threats with context-driven insights facilitates informed patching, mitigation, and risk decision-making	**Insightful Response** • Transform your exposure management practice with actionable, accessible, and understandable insights
Benefits	• Enhances data integrity across systems • Fosters team alignment by providing a standardized perspective, workflows, and methodology • Eliminates the reliance on spreadsheets for tracking	• Optimizes resource allocation, ensuring protection for your most critical assets • Leverage extensive threat integration and modeling, including mapping tactics, techniques, and procedures (TTPs) and MITRE ATT&CK™ to add essential context to a vulnerability	• Reports and dashboards offer deep security perspectives • Empowering stakeholders with a self-service portal that supports varied access controls • Accelerates decision-making

Take the first step!

Shifting to proactive exposure management as the first step of operationalizing your CTEM program is within reach. Ready to take the next step to quickly overcome your team's vulnerability-threat management gridlock and launch your journey? Schedule a demo with our exposure management experts today.



Ready for Phase 2 of Operationalizing for CTEM?

If you've successfully shifted from reactive to proactive vulnerability management, you're ready for the next phase of the Operationalizing for CTEM process- Optimizing for CTEM. This next phase will help clear critical hurdle that impede your ability to implement Gartner's continuous threat exposure management framework. Read the Optimize for Your CTEM Program brief here.